



DIR Office of the CISO
Texas Administrative Code Chapter 202
Webinar Questions and Answers
July 22 and 23, 2014

Q: When will the new controls be published

A: The controls will be published at the same time as the rule, likely the October-November timeframe.

Q: Is that the first time we can review?

A: Yes. That is the schedule for the rule review.

Q: How does one download the crosswalk without having to input credentials?

A: Click cancel when prompted. You may have to do so several times.

Q: Can you provide an update on the GRC tool to document individual agency efforts related to information security controls?

A: The control catalog will be integrated into the GRC tool that is under development.

Q: Is there opportunity for agencies to pilot the GRC tool and the controls in general?

A: I will relay your name and information to Nancy Rainosek, who is leading our GRC effort. She will likely look for volunteers to pilot the system toward the end of the year.

Q: This is all new to me. I am a new IRM (sitting in on this for my new ISO). What resources are there to help me understand TAC 202 and NIST SP 800-53 (like Cliff notes)? Or do I just have to read TAC and NIST text in full?

A: While it is likely important to read TAC to gain the fullest understanding, we will offer training (at ISF and through our ISO training program) that would also provide background. Participation in the monthly Information Security Working Group forum will also keep you up to date on Statewide Information Security Program activities, as well the monthly DIR Cybersecurity Insights newsletter.



Q: If there is time, it would be interesting to hear how Brian/Eddie were able to lead the group to consensus and a wonderful final document on such a complicated topic.

A: Great question. Mainly, we had an informal rule that if you didn't like something, you couldn't just say I don't like that. If someone thought they had another approach, they had to defend it. But we also respected everyone's opinion, and each person brought a genuine desire to make the best product that we could get. So with that, everyone participated in producing the end result.

Q: Where can we get the presentation for reference?

A: We will publish it on the DIR website, along with the FAQ and a recording of this session. We will email the IRM and Security Officer distribution lists when they are published.

Q: Will the control catalog crosswalk be available on the website as well?

A: The crosswalk is available on the DIR website at https://www.dir.texas.gov/SiteCollectionDocuments/Security/Texas%20CyberSecurity%20Framework/DIR_Control_Crosswalk.xls

Q: Will there be any formal/informal training made available to new ISO hires (who may not be familiar with State policies) to help them navigate the new 202?

A: Yes. DIR is developing an education program for ISOs (new and experienced) that goes into basic security principles and a specific class on Texas rules / regulations. The education program is in development and will begin in the Fall of 2014.

Q: We see that ITCHE gets its review period, when do agencies get to review & comment?

A: Agencies are able to review during the public notice and comment period, once published in the Texas Register.

Q: Any consideration of ISO 27001 and ISO 27002 in the crosswalk?

A: Slight oversight in the production of the crosswalk. ISO 27002 will be added to the crosswalk in an upcoming revision.



Q: When will the new P1's be published?

A: The P1s are directly mapped to NIST 800-53 and are available in that document. For reference the full NIST 800-53 revision 4 document can be found at
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

Q: When will the mod & high controls be added?

A: For the statewide security standards we will only require low level controls. Individual controls at the Mod or High level will be considered and incorporated using the effective / required date, but we do not anticipate implementing the Mod or High level controls as a statewide requirement. The control standards catalog will include the controls as reference for agencies that need to address specific risks.

Q: Where online can this be viewed for others who were unable to attend

A: We will provide the recorded webinar link that will include the slides and incorporate the Q&A from both sessions tomorrow after the second session.

Q: I may not have heard it but where can one get a copy of the draft?

A: The draft of the rule and control standards catalog is currently in the rule review process and provided to ITCHE for comment and impact analysis. In October the draft will be made available for public review.

Q: Hope you say how to get the current draft of the control catalog.

A: By way of the state rule making process for review and publish of TAC 202, it will be made available during the public review and comment period in October after the ITCHE provides their feedback and assessment is addressed.

Q: Is there any guidance in the new TAC regarding the how we categorize information system impacts as Low/Moderate/High? Are these impacts agency defined?

A: We have not specifically defined the categorization, but have incorporated by reference the FIPS standard for categorization and have a published guideline. Guideline information can be found at
<https://www.dir.texas.gov/SiteCollectionDocuments/Security/Texas%20CyberSecurity%20Framework/D ataClassificationGuide.docx>

TAC 202 Overview Webinar
July 23, 2014
Compiled Question and
Answers



And

<https://www.dir.texas.gov/SiteCollectionDocuments/Security/Texas%20CyberSecurity%20Framework/DataClassificationTemplate.xls>

Q: Will DIR send out email notification of the posting when it goes to the Register?

A: We will notify the Security and IRM Distribution lists.